CLAIM AMENDMENTS

The listing of claims will replace all prior versions and listings of claims in the application.

1. (Currently Amended) A data processing device, comprising an electronic memory component, the data processing device comprising:

a plurality of at least two access-secured sub-areas, each having at least one assigned part of a parameter comprising at least one bit, the device configured such that the parameter of at least one sub-area is encrypted only in certain areas, depending on at least one further sub-area an encryption method is applied to fewer than all of said sub-areas; and

an encryption block, wherein said encryption block receives at least one assigned part of said parameter from at least one of said sub-areas and encrypts said part of said parameter.

2. (Currently Amended) The data processing device as claimed in claim 1, wherein the encrypted part of the parameter in a first of the at least two access-secured sub-areas is encrypted as a function of at least one part of the parameter of the further sub-area a second of the at least two sub-areas.

3. (Original) The data processing device as claimed in claim 2, wherein at least one of an input value to the function or a return value from the function is more than one bit wide.

4. (Original) The data processing device as claimed in claim 1, wherein the memory component comprises:

an erasable programmable read only memory,

an electrically erasable programmable read only memory or

a flash memory.

5. (Canceled)

6. (Currently Amended) A method of securing access to an electronic memory, comprising:

receiving, by a data processing device, a parameter, wherein the parameter is comprised of at least two parts, each part comprising at least one bit;

assigning, by said data processing device, said parts of the parameter into at least two access-secured sub-areas located in said data-processing device; and

encrypting, by said data processing device, at least one of said parts of the parameter, of at least one of a plurality of in said access-secured sub-areas of the electronic memory with an encryption method, wherein the parameter to be encrypted of the sub-area is encrypted only in certain areas to increase security of the electronic memory said encryption method is applied to fewer than all of said sub-areas.

7. (Currently Amended) The method as claimed in claim 6, wherein said part

of the parameter ~~to be encrypted of the sub-area~~ is encrypted as a function of at

least one part of the parameter ~~of a~~in at least one further sub-area.

8. (Original) The method as claimed in claim 7, characterized in that the

function is one-to-one.

9. (Currently Amended) The method as claimed in claim 6, wherein ~~the~~each

access-secured sub-area~~s are secured separately~~ is encrypted with a separate

encryption method.

10. (Currently Amended) A data processing device, comprising an electronic

memory component, comprising:

a ~~plurality of~~at least two access-secured sub-areas, each having at least one

assigned part of a parameter comprising at least one bit, the device configured such

that ~~the parameter of at least one sub-area is encrypted only in certain areas,~~

~~depending on at least one further sub-area~~an encryption method is applied to fewer

than all of said sub-areas, the data processing device utilized in at least one of:

a one smart card controller,

a reader integrated circuit, ~~or~~

a cryptography chipset, or

for application in at least one of audio or video encryption.

11. (Previously Presented) The data processing device as claimed in claim 1, wherein the at least one assigned parameter comprises an address.

12. (Previously Presented) The method as claimed in claim 6, wherein the at least one parameter comprises an address.

13. (New) The data processing device as claimed in claim 10, wherein the at least one assigned parameter comprises an address.

14. (New) The data processing device as claimed in claim 1, wherein said device encrypts at least one part of said parameter, but not all parts of said parameter.

15. (New) The method as claimed in claim 6, wherein at least one part of said parameter, but not all parts of said parameter, are encrypted.

16. (New) The data processing device as claimed in claim 10, wherein said device encrypts at least one part of said parameter, but not all parts of said parameter.